AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method comprising:

generating message digests on a client connected with a network, wherein the message digests uniquely identify contents of files stored on the client;

synchronizing contents of the client with a repository connected with the network based on contents of the message digests on the client and corresponding entries in a database of message digests stored on the repository;

verifying that the contents of the repository match the contents of the client; and

marking ~~copying to the repository~~ those contents of the client that did not match the contents of the repository for later copying to the repository.

2. (Previously Presented) The method of claim 1, further comprising storing the message digests on the client.

3. (Previously Presented) The method of claim 2, further comprising generating new message digests for the files on the client to be cached on the repository prior to data synchronization.

4. (Previously Presented) The method of claim 1, wherein the files stored on the client comprise a subset of the files stored on the client.

5. (Cancelled)

6. (Previously Presented) The method of claim 1, wherein the generating of the message digests comprises generating a cryptographic hash for each file to be synchronized.

7. (Previously Presented) The method of claim 6, wherein the cryptographic hash comprises 128 to 160 bits.

8. (Previously Presented) The method of claim 1, wherein the synchronizing of the contents of the client with a repository comprises:

generating a first message digest for a file stored on the client;

reading a second message digest from the database of message digests from the repository corresponding to the first message digest;

comparing the first message digest to the second message digest;

determining whether contents of the client match contents of the repository based on the comparing the first message digest to the second message digest;

copying files from the client to the repository if the files are not found on the repository or do not match the files found on the repository; and

updating the database of message digests on the repository by copying the message digest from the client to the database on the repository.

9. (Previously Presented) The method of claim 1, wherein the verifying that the contents of the repository match the contents of the client comprises:

generating a first cryptographic hash from a list of message digests for all files on the client to be cached on the repository;

generating a second cryptographic hash from the contents of the database of message digests from the repository;

comparing the first and second cryptographic hash; and

repeating client and repository synchronization if the first and second cryptographic hashes do not match.

10. (Currently Amended) A system comprising:

a repository server connected with a network, the repository server to function as a data repository on behalf of a client; and

the client connected with the repository server via the network, wherein the client is to

generate a plurality of message digests that each uniquely identify the content of a corresponding file stored on the client,

synchronize contents of the client with files stored in the repository server based on contents of the message digests on the client and a database of message digests stored on the repository,

verify whether the contents of the repository match the contents of the client[[;]], and

mark ~~copy to the repository~~ those contents of the client that did not match the contents of the repository for later copying to the repository.

11. (Previously Presented) The system of claim 10, wherein the generating of the plurality of message digests comprises performing a cryptographic hash for each file to be synchronized.

12. (Previously Presented) The system of claim 11, wherein the cryptographic hash comprises 128 to 160 bits.

13. (Previously Presented) The system of claim 10, wherein the client is further to:

read a first message digest generated on the client;

read a second message digest from the database of message digests from the repository corresponding to the first message digest;

compare the first message digest to the second message digest;

determine whether contents of the client match contents of the repository based on said comparing the first message digest to the second message digest;

copy files from the client to the repository if the files are not found on the repository or do not match the files found on the repository; and

update the database of message digests on the repository by copying the message digest from the client to the database on the repository.

14. (Previously Presented) The system of claim 10, wherein the client is further to:

generate a first cryptographic hash from the message digest on the client;

generate a second cryptographic hash from the database of message digests from the repository;

compare the first and second cryptographic hash; and repeat client and repository synchronization if the first and second cryptographic hashes do not match.

15. -19. (Cancelled)

20. (Currently Amended) A machine-readable medium having stored thereon data representing sets of instructions which, when executed by a machine, cause the machine to:

generate message digests on a client connected with a network wherein the message digests uniquely identify contents of files stored on the client;

synchronize contents of the client with a repository connected with the network based on contents of the message digests on the client and corresponding entries in a database of message digests stored on the repository;

verify that the contents of the repository match the contents of the client; and

mark ~~copy to the repository~~ those contents of the client that did not match the contents of the repository for later copying to the repository.

21. (Previously Presented) The machine-readable medium of claim 20, wherein the client stores the message digests.

22. (Previously Presented) The machine-readable medium of claim 21, wherein the client generates new message digests for all files on the client to be cached on the repository prior to data synchronization.

23. (Previously Presented) The machine-readable medium of claim 20, wherein the files stored on the client comprise a subset of all files stored on the client.

24. (Cancelled)

25. (Currently Amended) The machine-readable medium of claim 20, wherein the client generates a cryptographic hash for each file to be synchronized[[;]].

26. (Previously Presented) The machine-readable medium of claim 25, wherein the cryptographic hash comprises 128 to 160 bits.

27. (Previously Presented) The machine-readable medium of claim 20, wherein the client:

generates a first message digest for a file stored on the client;

reads a second message digest from the database of message digests from the repository corresponding to the first message digest;

compares the first message digest to the second message digest;

determines whether contents of the client match contents of the repository;

copies files from the client to the repository if the files are not found on the repository or do not match the files found on the repository; and

updates the database of message digests on the repository by copying the message digest from the client to the database on the repository.

28. (Previously Presented) The machine-readable medium of claim 20, wherein the client:

generates a first cryptographic hash from a list of message digests for all files on the client to be cached on the repository;

generates a second cryptographic hash from the contents of the database of message digests from the repository;

compares the first and second cryptographic hash; and repeats client and repository synchronization if the first and second cryptographic hashes do not match.